CLAIMS

What is claimed is:

1. A method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups;

measuring a normal operation value of at least one operating parameter of any of said groups; and

detecting a change in said value to indicate possible malicious software behavior within said network.

2. A method according to claim 1 wherein said measuring step comprises measuring a ratio of the number of messages sent within any of said groups and between any of said groups over a period of time.

3. A method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups;

identifying a known malicious software behavior pattern for any of said groups;

determining a normal behavior pattern for any of said groups;

setting a threshold between said normal and malicious software behavior patterns; and

detecting behavior is detected that exceeds said threshold.

4. A method according to claim 3 and further comprising performing a malicious software containment action if behavior is detected that exceeds said threshold.

5. A method according to claim 3 wherein any of said patterns are expressed as any of a numbers of message per unit of time, a shape of a utilization graph, a graph of e-mail messages per unit of time, a histogram of communication frequency vs. proximity measure, a number of messages sent within any of said groups, number of messages sent from one of said groups to a another one of said groups, and a histogram of e-mail lengths.

6. A method according to claim 3 and further comprising notifying at least one neighboring group of said group in which said threshold is exceeded.

7. A method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups;

identifying activity suspected of being malicious occurring sequentially in at least two of said groups between which a proximity measure is defined; and

searching for communication events between said at least two groups which are associated with the progress of malicious software from the first of said at least two groups to the second of said at least two groups.

8. A method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups;

identifying generally simultaneously suspicious malicious activity in at least two of said groups between which a proximity measure is defined; and

identifying a generally similar communication received by said groups.

9. A method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups;

collecting information regarding target behavior detected at any of said computing devices;

correlating said target behavior within said groups; and

determining whether said correlated target behavior information corresponds to a predefined suspicious behavior pattern.

10. A method according to claim 9 wherein said grouping step comprises grouping such that malicious software will spread according to a predefined spread pattern relative to said groups.

11. A method according to claim 9 and further comprising performing at least one malicious software containment action upon determining that said correlated target behavior information corresponds to a predefined suspicious behavior pattern.

12. A method according to claim 9 wherein said grouping step comprises grouping according to a measure of proximity.

13. A method according to claim 12 wherein said measure of proximity is a measure of logical proximity.

14. A method according to claim 13 wherein said measure of logical proximity is a frequency of communication between at least two computing devices.

15. A method according to claim 12 wherein said grouping step comprises applying a clustering algorithm to said measure of logical proximity.

16. A method according to claim 9 and further comprising:

replacing any of said groups with a node operative to aggregate all communications between said computing devices within said replaced group.

17. A method according to claim 9 and further comprising identifying a plurality of neighboring ones of said groups.

18. A method according to claim 9 and further comprising applying a clustering algorithm to identify a plurality of neighboring ones of said groups.

19. A method according to claim 17 and further comprising, upon detecting suspect malicious software activity in any of said groups, notifying any of said neighboring groups of said suspect malicious software activity.

20. A method according to claim 19 and further comprising any of said neighboring groups using, in response to said notification, the same sensing mechanisms as said group from which said notification was received

21. A method according to claim 9 wherein any of said groups employs a live set of malicious software sensors and a test set of malicious software sensors.

22. A method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups;

receiving messages sent from any of said computing devices;

buffering any of said messages received from any of said computing devices in one of said groups and destined for any of said computing devices in a different one of said groups for a predetermined delay period prior to forwarding said messages to their intended recipients.

23. A method according to claim 22 wherein said delay period is dynamic.

24. A method according to claim 22 wherein said delay period is adjustable according to a level of suspicious behavior in any of said groups.

25. A method according to claim 22 wherein said buffering step comprises separately buffering messages sent within any of said groups and messages sent outside of any of said groups.

26. A method according to claim 22 and further comprising performing at least one malicious software containment action upon said buffer.

27. A method according to claim 22 wherein said grouping step comprises grouping according to a measure of proximity.

28. A method according to claim 27 wherein said measure of proximity is a measure of logical proximity.

29. A method according to claim 28 wherein said measure of logical proximity is a frequency of communication between at least two computing devices.

30. A method according to claim 27 wherein said grouping step comprises applying a clustering algorithm to said measure of logical proximity.

31. A method according to claim 22 and further comprising:

replacing any of said groups with a node operative to aggregate all communications between said computing devices within said replaced group.

32. A method according to claim 22 and further comprising identifying a plurality of neighboring ones of said groups.

33. A method according to claim 22 and further comprising applying a clustering algorithm to identify a plurality of neighboring ones of said groups.

34. A method according to claim 32 and further comprising, upon detecting suspect malicious software activity in any of said groups, notifying any of said neighboring groups of said suspect malicious software activity.

35. A method according to claim 34 and further comprising any of said neighboring groups using, in response to said notification, the same sensing mechanisms as said group from which said notification was received

36. A method according to claim 22 wherein any of said groups employs a live set of malicious software sensors and a test set of malicious software sensors.

37. A method for malicious software detection comprising:

grouping a plurality of computing devices in a network into at least two groups;

configuring each of said groups to maintain a malicious software detection sensitivity level; and

upon detecting suspected malicious software activity within any of said groups, notifying any other of said groups of said detected suspected malicious software activity.

38. A method according to claim 37 and further comprising:

adjusting said malicious software detection sensitivity level at any of said notified groups according to a predefined plan.

39. A method according to claim 37 wherein said grouping step comprises grouping according to a measure of proximity.

40. A method according to claim 39 wherein said measure of proximity is a measure of logical proximity.

41. A method according to claim 40 wherein said measure of logical proximity is a frequency of communication between at least two computing devices.

42. A method according to claim 39 wherein said grouping step comprises applying a clustering algorithm to said measure of logical proximity.

43. A method according to claim 37 and further comprising:

replacing any of said groups with a node operative to aggregate all communications between said computing devices within said replaced group.

44. A method according to claim 37 and further comprising identifying a plurality of neighboring ones of said groups.

45. A method according to claim 37 and further comprising applying a clustering algorithm to identify a plurality of neighboring ones of said groups.

46. A method according to claim 44 and further comprising, upon detecting suspect malicious software activity in any of said groups, notifying any of said neighboring groups of said suspect malicious software activity.

47. A method according to claim 46 and further comprising any of said neighboring groups using, in response to said notification, the same sensing mechanisms as said group from which said notification was received

48. A method according to claim 37 wherein any of said groups employs a live set of malicious software sensors and a test set of malicious software sensors.

49. A method for malicious software detection, the method comprising:

collecting information regarding target behavior detected at any of a plurality of computers;

correlating said target behavior; and

determining whether said correlated target behavior information corresponds to a predefined suspicious behavior pattern.

50. A method for malicious software detection, the method comprising:

receiving messages sent from a computer; and

buffer any of said messages received from said computer for a predetermined delay period prior to forwarding said messages to their intended recipients.

51. A method for malicious software detection, the method comprising:

configuring each a plurality of servers to maintain a virus detection sensitivity level; and

providing multiple pluralities of computers, each plurality of computers being in communication with at least one of said servers;

detecting suspected virus activity at any of said plurality of computers, and

notifying any of said servers of said detected suspected virus activity.